

Lending Standards Board

Call for Input

**Contingent Reimbursement Model Code for
Authorised Push Payment Scams**

March 2021

Contents

1. Executive Summary.....	3
2. Introduction	5
a. Context of current work: regulatory developments	6
3. The Call for Input: Topics Raised	7
a. The evolving nature and complexity of APP scams and the CRM Code	7
b. Wider participation of firms in the CRM Code	8
c. Roles and responsibilities in the CRM Code	10
d. The customer experience and the role of firms along payment journeys	11
4. Next Steps	14
a. How to respond	14
5. Appendix.....	15
Summary of questions.....	15

1. Executive summary

The Lending Standards Board's (LSB) mission is to drive fair customer outcomes within financial services through independent oversight. The LSB is the primary self-regulatory body for the banking and lending industry. Our registered firms comprise the major UK banks and lenders, credit card providers, debt collection agencies and debt purchase firms.

In January 2021, the LSB published the first [full review](#) of the Contingent Reimbursement Model Code for Authorised Push Payment Scams (the Code) since becoming responsible for the governance of the Code in July 2019. This Call for Input follows on from the key recommendations within that report.

The full review considered how the Code has been implemented by firms, adopted into the wider payments landscape, and where improvements are required to the Code to ensure greater consistency in its application. It encompassed a broad evidence base including previous LSB thematic reviews, a public consultation, analysis of data from signatory firms and ongoing engagement with stakeholders. The review then set out recommendations, to be taken forward by the LSB and stakeholders, to ensure that the Code and the consumer protections which sit at the heart of it work effectively.

The recommendations included introducing Code provisions around Governance and Oversight, with a view to ensuring it is implemented consistently and is embedded into a signatory firm's culture; defining success measures of the Code which evidence aspects beyond reimbursement; and exploring the expansion of the scope of the Code so that it is inclusive of a greater diversity of firms in the payments landscape and takes account of emergent APP scams which are employing ever more sophisticated methods to defraud customers. Related to this, we committed to further explore the responsibilities on sending and receiving firms, as well as the role of other potential firms on the payment supply chain.

At the stage of issuing our report, we did not have sufficient evidence submitted to us to formulate decisions which would help shape policy on a number of specific topics. We have therefore issued the current Call for Input to explore those topics further, specifically focusing on the following:

- That the scope of the Code should more fully reflect the evolving nature and complexity of Authorised Push Payment (APP) scams to ensure that it is able to remain relevant and in line with developments in the wider payments landscape.
- That the Code should recognise the wider range of participants within the payments industry whilst ensuring that it retains a consistent approach to the standards of protections provided. This included considering the wording of the Code at SF1(3) so that the provision becomes effective within the Code for those firms who have implemented Confirmation of Payee (CoP).
- That the Code should more fully reflect the roles and responsibilities of receiving firms in the customer payment journey. Related to this we also want to explore how the Code can balance responsibilities of parties in the payment journey, especially where this goes beyond the traditional three-party payment model. As part of this we also want to better understand how consumers navigate the payments landscape, particularly where they are undertaking payments that go beyond the three-party model, and consumer behaviour with regards to seeking remedy where they have been scammed in more complex payment supply chains.

This document forms part of range of activity the LSB is undertaking following the publication of our report. Further information is set out in our [roadmap](#). We would encourage respondents to this Call for Input to read this document in conjunction with the wider work we have undertaken on the Code, in particular the [full review](#) published in January.

2. Introduction

On 28 January 2021, the Lending Standards Board (LSB) published its report of the review into the CRM Code, following an industry-wide consultation.

The current Call for Input should be read as a follow up to our full [review](#), which assessed how the Code is working, and sought views on how it has been implemented and what further improvements may be required to ensure its effectiveness.

In addition to the recommendations outlined in our review, there were some topics which were identified as being potentially detrimental to consumers, and which it was felt that the Code did not adequately cover. These are the subject of the current Call for Input. We do not intend for the current document to repeat the issues already covered in the full review, but instead to home in on specific topics for which there was not sufficient evidence submitted in the full review, so that we could form policy and Code decisions. We are therefore seeking further information on the following topics:

- **That the scope of the Code should more fully reflect the evolving nature and complexity of APP scams.** At present it covers first generation accounts whereby a consumer transfers funds straight to the scammer's account. Accounts used in the onward transmission of funds are beyond the Code scope.
- **That the Code should recognise the wider range of participants within the payments industry.** As consumers choose to conduct payments using various methods and firms, we want to ensure consumer protections against APP scams are available to all, irrespective of the firm the consumer chooses to transact with. We want to explore extending Code protections to the consumers of firms such as Building Societies, Payment Initiation Service Providers (PISPs), electronic money issuers and other newer participants offering payment options and services.

Within this, we also committed to reviewing the wording of the CoP provisions in the Code so that the provision becomes effective for those firms who have implemented it. At present, this continues to remain in a holding position, contingent upon the progress of Pay.UK's work, whom we continue to engage with.

- **That the Code should more fully reflect the roles and responsibilities of receiving firms.** Related to this, we also want to explore how the Code can balance responsibilities of parties in the payment journey, especially where this goes beyond the traditional three-party payment model. As part of this we also want to better understand how consumers navigate the payments landscape, particularly where they are undertaking payments that go beyond the three-party model, and consumer behaviour with regards to seeking remedy where they have been scammed in more complex payment supply chains.

Who should respond?

We are keen to hear from as many stakeholders and those impacted by the Code as possible. This includes Code signatories and other firms providing payment services to consumers, consumer representatives, and the industry more generally.

While we have set out a range of questions in this consultation, further comment, discussion, and representations from respondents is encouraged in respect of any of the recommendations made within our full review. Respondents are welcome to provide supporting documents for their views.

The details of how to respond to this consultation are set out in section 4, Next Steps. We would welcome responses to the questions raised in this consultation and any related feedback by 5pm on 26 May 2021.

a. Context of current work: regulatory developments

As referenced within our January report, we recognise that we are undertaking our work against a backdrop of wider regulatory activity. There is ongoing work looking at the payment landscape by HM Treasury, and since the publication of our report, the Payment Systems Regulator (PSR) and Open Banking Implementation Entity (OBIE) have initiated consultation processes related to the CRM Code and APP scams more generally.

Payment Systems Regulator: CP21/3 Authorised Push Payment (APP) Scams, Call for Views: In February 2021, the PSR launched a [call for views](#) on APP scams within which the regulator also discusses its views on the CRM Code. The PSR's call for views seeks to establish views on the viability, effectiveness, and proportionality of several complementary measures proposed in the document which the regulator believes will help to deter APP scams and lessen the impact when they do occur.

Open Banking Standards re: Confirmation of Payee and CRM Code consultation: The Open Banking Implementation Entity launched a [consultation](#) on evolving Open Banking standards with regards to Confirmation of Payee and the CRM Code for PISPs. The OBIE is seeking views on establishing CoP and the CRM Code in the PISP payment journey. Alongside this consultation, the OBIE also launched consumer research on effective warnings.

Pay.UK is the Recognised Payment System Operator for the Bacs and Faster Payments systems and manages the Confirmation of Payee service. While some firms beyond the six banking groups directed by the PSR have voluntarily introduced CoP, we are mindful that not all firms have done so. We understand that Pay.UK and industry are continuing to work on the next phase of CoP, which will enable more firms to implement this fraud-prevention tool. As the Code currently stands, there is a holding date for the CoP provision to be made effective.

The Code provisions related to CoP remains subject to the progress of this work. It is important to ensure that the implementation of the CoP provision would not mean that firms who have not yet adopted CoP, or who fall within phase two of Pay.UK's work in this area, are in breach of the Code, or that the provision creates a further barrier to entry for non-signatories. We therefore continue to liaise with Pay.UK throughout the course of our work.

It is against this wider background of developments that we are progressing with our CRM Code activity¹ and conducting ongoing engagement to ensure we remain cognizant of developments in the payment's environment.

3. The Call for Input: Topics Raised

a. The evolving nature and complexity of APP scams and the CRM Code

The Code applies to the movement of funds from the customer's account to an account controlled by the scammer (the first-generation account). Once received, funds will be quickly moved onwards by the scammer, to potentially several accounts.

For the purposes of the Code, firms whose accounts are utilised in the onward transmission of APP scam funds are out of scope². There was some anecdotal evidence provided via consultation responses which suggested that APP scams are evolving in sophistication, for example, increasing the number of transactions or payees involved in the scam, making it more difficult for firms to track and freeze the funds, or changing methods to perpetrating the scams which may not be captured by the Code as it currently stands.

The evidence submitted to us was limited but given the potential for customer detriment, the evolving nature of APP scams and how they are considered within the scope of the Code requires further consideration. From some of the information submitted to us, we saw that such emergent scams were utilising techniques which were not adequately captured by the Code; for example, elongating the payment supply chain or incorporating a range of payment methods within the scam.

There was a view that the three party model outlined in the Code cannot fully account for such techniques. The three party model refers to how at present, the Code recognises that there are three parties involved in the payment journey: the customer as they authorise the payment; the customer's firm (the sending firm); and the receiving firm (the account to which the money is moved). It sets out that the sending firm is responsible for the assessment of any claim made under the Code.

This model assumes that the customer who has been scammed (and likely socially engineered) will report this to their bank and the processes set out in the Code will begin at that point. However, where funds have transitioned through other accounts before moving onto the account under the scammer's control, it may not always be the ultimate customer (the person who has fallen victim to the scam) who alerts their firm. In such cases, this poses questions with regards to how, and where, the Code applies.

Given the rewards, those who perpetrate APP scams will continue to evolve approaches and techniques to ensure that they are able to exploit gaps both in consumer awareness around APP scams and the systems and controls implemented by the industry to address them. As the payments journey and movement of funds becomes more complex, involving a wider range of participants, the attribution of responsibility for the consequent remedial actions may become less clear, and may move beyond the scope of current Code protections. It is therefore important that we, along with industry, regulators, and customers, are aware of and understand the nature of such emerging scams, their prevalence, and the customer experience in such payment journeys.

¹ We have created a [roadmap](#) of CRM Code review activities to highlight our workplans on this in 2021

² Provision DS2(1)(b) CRM Code is also between GBP-denominated UK-domiciled accounts.

Questions

1. Please tell us about any APP scams which you have encountered, and which you perceive do not fit into the Code adequately?
 - a. Please describe the nature and volume of such scams.
 - b. Were Code provisions applied to such cases? If so, please describe how Code provisions were applied and describe any other aspects of the Code which impacted on such cases.
 - c. Do you have views on how the Code should be amended to help the prevention of such scams or mitigate their impact?
2. Are you aware of any resolution that was sought by the victims of such scams? How did they go about this? What was the outcome?

b. Wider participation of firms in the CRM Code

As financial services and the payments ecosystem continue to evolve, business models outside of traditional banking structures have developed to serve customers' financial and payment needs. Against the backdrop of this evolution, it is vital that protections are afforded to as many customers as possible who use both traditional and newer banking and payment models.

For the Code to work as effectively as possible, it should reflect the range of firms operating within the payments system. Involving more stakeholders in the payments ecosystem to work collaboratively will have a number of advantages: improved and greater levels of intelligence about APP scams; a greater number of consumers are protected; better communication between firms; and expedient remediation, to name but a few.

Responses to our consultation suggested that the Code was perceived to be designed for larger firms with little analysis on how it is commensurate with consumer protection policies and initiatives which other types and sizes of firms already undertake. This feedback related, in the main, to business models of Building Societies, Payment Initiation Service Providers (PISPs) and Electronic Money Issuers.

Feedback suggested that the types of firms mentioned do desire to participate in the Code, however barriers were cited which were perceived to prohibit full participation in the Code by certain types of firms. In addition to responses received from the previous consultation, we have also engaged with specific sectors to better understand their views on the Code provisions.

From this engagement activity, some common barriers identified included:

- Behavioural analysis was said to be difficult where transaction volumes are typically low which creates challenges in being able to create a meaningful customer profile.
- Technology changes required to introduce additional controls/warnings can be a challenge for firms, particularly those at the smaller end of the scale or those with limited in-house IT resources.
- Feedback on the ability to identify customers who may be deemed vulnerable to APP scams focused on the concerns around the inability for some firms to adhere to provisions around detection and utilising intelligence about customers and transactions. This is particularly the case for firms that enable one-time and specific

payments or do not hold a continuous customer relationship, therefore historical transactional data may not be available in the same way it is, for example, for current account providers.

- The ability to provide dynamic warnings was said to be difficult to achieve in the absence of transactional or behavioural data to determine which warning should be presented to the customer.
- The ability to provide a 24/7 contact option was said to be challenging where, for example, there is not an existing option for customers to contact their firm out of office hours.
- The ongoing uncertainty around the status of the no blame fund³.
- The ability to collate and provide statistics on APP scams to their relevant trade body was considered a challenge, as currently, only UK Finance collates these statistics on behalf of its members.

There was also some feedback which suggested that participation in the Code was not necessary for such firms to offer their customers protection against APP scams. This was based on the view that the scam risk exposure for such firms was lower than current Code signatories, and therefore some firms felt the Code was too onerous in proportion to the level of APP scams occurring within their respective organisations. To comply with the Code, it was suggested that these types of firms would need to invest considerable resource to build additional functionality and friction within their systems, as well as training staff and operationalising the Code. Moreover, it was suggested that consumer protection initiatives already existed within their own industry sectors, which are as effective as the consumer protections afforded by the Code.

Whilst recognising the benefits of increased coverage of the Code, we are mindful that any proposed amendments to the Code to remove some or all the current barriers to sign-up do not inadvertently reduce the consumer protections in place.

Implementation of Confirmation of Payee

In addition to the barriers cited above, some respondents also cited their inability to comply with the CoP provisions within the Code. As the Code currently stands, provision SF1(3) has a holding date for the implementation of CoP. This functionality elicited strong support in the majority of consultation responses, with the recognition that whilst CoP is not a panacea to the prevention of all APP scams, it nonetheless provides protection by design.

Whilst CoP is in place across most signatory firms, it has yet to be made effective within the Code. Implementing the CoP provision in the Code would mean that whether the customer took heed of the CoP outcome could be considered during firms' subsequent assessment process.

However, we are also mindful that not all signatories to the Code were subject to the PSR's direction. It will therefore be important to ensure that the implementation of the Code provision would not mean that firms who have not yet adopted CoP, or who fall within phase two of Pay.UK's work in this area, are in breach of the Code, or that the provision creates a further barrier to entry for non-signatories. Subject to the above considerations, we did not receive any feedback which suggested that CoP should not be made effective within the Code.

³ Within the review document, we addressed this by committing to update Provision ALL2(3) of the Code to reflect that firms may fund no blame cases from the central fund or 'self-fund' the reimbursement of customers who are assessed to be in a 'no blame' scenario.

As part of our Call for Input, we intended to set out a date for implementation of CoP within the Code. However, we understand that Pay.UK phase two activity has not yet concluded and therefore the date for implementation of the Code provision cannot be set. We will endeavour to do this as soon as possible.

Questions

3. Do you have views on whether there should be a priority amongst firms with regards to Code participation? Please explain your view.
 - a. Are there other business models not mentioned to whom the Code would be of relevance?

4. If you are a non-signatory firm, please tell us about your business model and your inclination to be a signatory to the Code.
 - a. Are there additional barriers to the ones cited above that we should be aware of?
 - b. If so, what changes to the Code would be needed to accommodate your business model?
 - c. If these changes were addressed, how likely are you to become a signatory?
 - d. Please tell us about the steps you currently take, or sector initiatives you participate in, which offer consumer protections against APP scams for your customers. Please also tell us about any APP scams you encounter and your current processes for resolving them.

c. Roles and responsibilities in the CRM Code

As stated earlier, the Code works to the three-party model whereby it recognises the customer, the customer's firm (as the sending firm) and the receiving firm (the account to which the money is moved). The Code further sets out that the sending firm is responsible for assessment of claims made under the Code.

Feedback from existing signatories, as well as consumer representatives, suggested that responsibilities between sending and receiving firms that are signatories to the Code should be reviewed, with the intention of placing greater emphasis on the role of the receiving firms. There was a general view that receiving firms have less responsibility under the Code and related to this, there were questions raised around the equitable balancing of responsibilities between sending and receiving firms.

The need to balance responsibilities was suggested to drive greater prevention activity, for example, improving the processes which allow for the communication between firms; the associated freezing of funds; and the repatriation processes which can only take place once a receiving bank has been notified of a suspected APP scam case.

There was also a view that receiving firms should take more responsibility as funds were being transferred to accounts which had been either allowed to be opened without the adequate checks, or the account was being allowed to be used without proper interventions for account holders who act, or are coerced to act, as money mules⁴. This was clearly viewed as an area that only the receiving bank could have proper influence over, given the account where funds

⁴ These are legitimate accounts used in the onward transmission of the proceeds of APP scams

were being received was held with them. On the issue of tackling money mule fraud, the banking and finance industry has taken a number of steps, including:

- Deterring young people from becoming money mules through the Don't Be Fooled campaign, run jointly by UK Finance and Cifas.
- Funding the Dedicated Card and Payment Crime Unit (DCPCU), a specialist police force that targets the criminal gangs behind fraud. The DCPCU has worked with social media companies to take down 732 accounts linked to fraudulent activity in 2020, of which 258 were involved in recruiting money mules.
- Working with Pay.UK to implement the Mule Insights Tactical Solution (MITS), a technology that helps to track suspicious payments and identify money mule accounts.⁵

Highlighting the role of receiving firms and the increased focus on addressing mule accounts demonstrate that APP scams are complex in nature and prevention activity needs just as much focus as resolution. Greater involvement and cooperation by receiving firms would strengthen this preventative element, as well as help to expediate the resolution for scammed customers. We are therefore keen to understand the role of receiving firms in APP cases, both as it stands and particularly the experiences of customers as they deal with different parties in the customer journey, with a view to assessing how the Code can help in this process.

Questions

5. Do you have views about the experience of customers in their dealings with sending and receiving firms when they have reported an APP scam?
6. Do you have a view on how the responsibilities between sending and receiving firms are laid out in the Code?
7. Are there any changes to the Code you believe would help to resolve any imbalances in sending or receiving firm responsibilities?

d. The customer experience and the role of firms along payment journeys

At the heart of any payment supply chain is the consumer. As with discussions around the responsibilities of receiving firms under the Code, we need to continue to understand the customer experience throughout the payment journey, so that protections are designed which best meet consumer needs.

It is right that customers have a choice about how they want to transact, and that a diversity of firms are given the opportunity to innovate and extend their payment products and services which are best suited to serve consumer needs. We would like to see the high standards of consumer protections within the Code extended to as many customers as possible without restriction of consumer choice or payment innovation. The balance to be struck in this regard inevitably raises questions around how responsibilities of the Code are attributed amongst the participants involved in the payment transaction.

⁵ <https://www.ukfinance.org.uk/press/press-release/money-mule-recruiters-use-fake-online-job-adverts-to-target-generation-covid>

During our review, we received feedback from organisations representing consumer interests, which evidenced gaps in communications by firms with customers who contacted them once they realised, they had been scammed. There were also further issues with lack of clarity and information provided in decisioning letters and correspondence received from firms. This was exacerbated by concerns regarding a lack of awareness about the Code by frontline staff. This echoed our findings which are discussed in detail, in both the January report and our themed review of R2(1)(c), where it was identified that further work was required to ensure that customers were aware of the basis on which the decision had been made to decline reimbursement and the support which is available to those who have fallen victim to scams. In line with the LSB's oversight framework, we issued individual reports to firms which contained recommendations and required actions identified during the review. We are continuing to work with firms to ensure that these are implemented. Work is also underway on the follow up review on provision R2(1)(c) to ensure that firms have addressed and implemented the recommendations and actions previously identified.

In this section however, we want to go beyond consumer communications with just their own firm and try to understand consumer interactions along the whole payment supply chain. These issues are even more pertinent where multiple firms might be involved in a payment transaction, such as in scenarios where a customer conducts a payment transaction which involves their own firm and a PISP. An example of one such payment is where a customer purchases goods from a website and authorises a PISP to transfer money from their bank account to pay for these, instead of using their debit card. If a scam were to occur on such payment journeys, we want to better understand processes and interactions with all parties in these contexts. We are particularly interested to hear how consumers understand their avenues to recourse in such circumstances.

We also received feedback at the last review that organisations representing consumers had the potential to play a greater role in the payment supply chain where a customer is scammed, and that this role should be captured within the Code. The roles suggested ranged from being signposted to sources of help within the payment journey, through to being advocates and conducting communications with banks on behalf of consumers who have fallen victim to an APP scam. We want to better understand what these roles may look like, and what the associated benefits and drawbacks may be, with a view to understanding how the Code may impact this.

Questions

8. Do you have views on Code provisions and how they relate to the role of different firms on the payment journey?
9. Do you have views about how consumers understand their responsibilities and rights when they are undertaking a payment, particularly in circumstances involving more complex payments (e.g. including PISPs)?
 - a. Who do scammed consumers contact in such circumstances? If you have examples of where consumers have interacted with different firms after reporting a scam, please share with us.
10. What roles do you think organisations representing consumers who have been scammed, can play in the payment supply chain? Please outline any barriers and enablers you see to such roles.

11. Do you have views on how Code responsibilities should be attributed along the payment journey?

4. Next Steps

a. How to respond

Code signatories, other firms, consumer representatives and the industry more generally will have an interest in the topics covered within this Call for Input, and we would encourage responses from anyone affected by these issues.

The full list of questions can be found in the Appendix to this document. While we have set out a range of questions in this document, further comment, discussion, and representations from respondents are encouraged in respect of any of the elements of the Code or the supporting documents.

We would encourage respondents to share any insight and evidence they can that supports their response to this consultation, even if this can only be done on a confidential basis. Respondents are also welcomed to provide suggestions for changes to the Code or the supporting documents.

The responses to the Call for Input and the work undertaken as part of the wider progression of recommendations may be used to inform revisions to the Code and to the supporting documents that fall within the scope of our review.

We would welcome responses to the questions raised in this consultation and any related feedback by 5pm on 26 May 2021. Responses submitted after this date may not be considered.

Please send your responses to: crmcode@lstdb.org.uk

Publication of responses

From experience, we know that many of the responses submitted will likely include sensitive operational information and will be provided on a confidential basis. We are grateful for the openness of these responses and the nature of the information provided which allows us to look in-depth at the workings of the Code. Given the highly sensitive nature of many of the previous responses on this topic, we have taken the decision not to publish responses we receive to this Call for Input.

The Code and this document do not contain any legal advice to any person or firm and is no substitute for formal legal advice required by any person or firm. The LSB does not accept any legal responsibility or liability for the actions or omissions of any person or firm in relation to or reliance on the Code or this consultation document.

5. Appendix

a. Summary of questions

3.a The evolving nature and complexity of APP scams and the CRM Code

1. Please tell us about any APP scams which you have encountered, and which you perceive do not fit into the Code adequately?
 - a. Please describe the nature and volume of such scams.
 - b. Were Code provisions applied to such cases? If so, please describe how Code provisions were applied and describe any other aspects of the Code which impacted on such cases.
 - c. Do you have views on how the Code should be amended to help the prevention of such scams or mitigate their impact?
2. Are you aware of any resolution that was sought by the victims of such scams? How did they go about this? What was the outcome?

3.b Wider participation of firms in the CRM Code

3. Do you have views on whether there should be a priority amongst firms with regards to Code participation? Please explain your view.
 - a. Are there other business models not mentioned to whom the Code would be of relevance?
4. If you are a non-signatory firm, please tell us about your business model and your inclination to be a signatory to the Code.
 - a. Are there additional barriers to the ones cited above that we should be aware of?
 - b. If so, what changes to the Code would be needed to accommodate your business model?
 - c. If these changes were addressed, how likely are you to become a signatory?
 - d. Please tell us about the steps you currently take, or sector initiatives you participate in, which offer consumer protections against APP scams for your customers. Please also tell us about any APP scams you encounter and your current processes for resolving them.

3.c Roles and responsibilities in the CRM Code

5. Do you have views about the experience of customers in their dealings with sending and receiving firms when they have reported an APP scam?
6. Do you have a view on how the responsibilities between sending and receiving firms are laid out in the Code?
7. Are there any changes to the Code you believe would help to resolve any imbalances in sending or receiving firm responsibilities?

3.d The customer experience and the role of firms along payment journeys

8. Do you have views on Code provisions and how they relate to the role of different firms on the payment journey?
9. Do you have views about how consumers understand their responsibilities and rights when they are undertaking a payment, particularly in circumstances involving more complex payments (e.g. including PISPs)?

- a. Who do scammed consumers contact in such circumstances? If you have examples of where consumers have interacted with different firms after reporting a scam, please share with us.

10. What roles do you think organisations representing consumers who have been scammed, can play in the payment supply chain? Please outline any barriers and enablers you see to such roles.

11. Do you have views on how Code responsibilities should be attributed along the payment journey?